



To: Card Program Administrators
From: U.S. Bank Corporate Payment Systems
Re: SECURITY ALERT - FRAUDULENT CARDHOLDER EMAILS

We have had reports from cardholders that they are receiving requests via email that appear to come from U.S. Bank. The email claims that the recipient's accounts have been blocked and asks the recipient to enter his or her account number and other personal information.

According to U.S. Bank's Fraud Prevention and Investigation area, this is a fraudulent email and did not come from U.S. Bank. Their instructions to recipients are **DO NOT REPLY** to this email under any circumstances and furthermore, do not click on the link in this email.

U.S. Bank will not contact cardholders directly under any circumstances to verify account numbers or personal information. This is an excellent time to remind cardholders that if they ever receive a request like this via email or telephone, they should not respond.

We would also like to assure all clients that there has been no fraudulent activity reported and no cards have been suspended as this email suggests. There was no breach of any secure account information. These emails are random and are being sent using a spam list that includes individuals who in many cases do not even have U.S. Bank accounts. Similar email fraud campaigns have been reported using names of other banks, too.

Reporting Fraudulent Email

U.S. Bank and the Federal Bureau of Investigation (FBI) are working diligently to stop these illegal activities. To help track these cyber-criminals, the U.S. Bank Fraud Department is requesting that anyone who has received a suspicious email send a copy of it to fraud_help@usbank.com, along with their responses to the questions below.

- Do you have an account relationship with U.S. Bank?
- What Internet Service Provider (ISP) do you use?
- What type of connection do you use to access the Internet? Cable, dialup, DSL or other?
- Do you have a firewall installed on your computer?